COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the SAF/AAD WWW site at: http://afpubs.hq.af.mil. If you lack access, contact your Publishing Distribution Office (PDO).

This instruction implements Air Force Policy Directives (AFPD) 33-1, *Command, Control, Communications, and Computer (C4) Systems*, and 33-2, *Information Protection*. This instruction prescribes the requirements, responsibilities and procedures for the security program for the Strategic Automated Command Control System-Data Transmission Subsystem (SACCS-DTS). It applies to all users and personnel employing the SACCS-DTS Network, either through direct input or interface systems. Provide a copy of all major command (MAJCOM) and field operating agency (FOA) supplements to Headquarters Air Force Space Command (HQ AFSPC)/SCMB, 150 Vandenberg St, Ste 1105, Peterson AFB CO 80914-4730, with a copy to Headquarters Air Force Communications Agency (HQ AFCA)/XPXP, 203 W Losey Street, Room 1060, Scott AFB IL 62225-5233. Refer recommended changes and conflicts between this and other publications to HQ AFSPC/SCMB, using AF Form 847, **Recommendation for Change of Publication**, with an information copy to HQ AFCA/XPXP.

SUMMARY OF REVISIONS

This is the initial publication of Air Force Instruction (AFI) 33-107, Volume 2.

1. Applicability, Terminology, and References.

   1.1. **Applicability.** This instruction applies to all users that interface with or support the Strategic Automated Command Control System, Data Transmission Subsystem (SACCS-DTS) Network. It provides commanders with information required for decisions affecting the control and direction of operational forces. In addition, it provides subscribers with direct interface to the Automatic Digital Network (AUTODIN), Air Force Global Weather Center (AFGWC), Command Center Processing and Display System (CCPDS), Air Force Satellite Communications (AFSATCOM), and Survivable

Report Documentation Page

Report Date	Report Type	Dates Covered (from... to)
01 Nov 1997	N/A	-

Title and Subtitle	Contract Number
Air Force Instruction 33-107, V2, Communications and Information, Strategic Automated Command Control System-Data Transmission Subsystem (SACCS-DTS) Network Security Program	**Grant Number**
	Program Element Number

Author(s)	Project Number
	Task Number
	Work Unit Number

Performing Organization Name(s) and Address(es)	Performing Organization Report Number
Secretary of the Air Force Pentagon Washington, DC 20330-1250	AFI33-107V2

Sponsoring/Monitoring Agency Name(s) and Address(es)	Sponsor/Monitor's Acronym(s)
	Sponsor/Monitor's Report Number(s)

Distribution/Availability Statement
Approved for public release, distribution unlimited

Supplementary Notes

Abstract

Subject Terms

Report Classification	Classification of this page
unclassified	unclassified

Classification of Abstract	Limitation of Abstract
unclassified	UU

Number of Pages
23

Low Frequency Communications System (SLFCS). SACCS is two major electronically interconnected subsystems—the DTS and the Data Processing Subsystem (DPS).

1.1.1. Authority And Organization. HQ AFSPC, as the lead command of the SACCS-DTS Network, has responsibility for operations guidance, hardware configuration, and software maintenance. The 55th Computer Systems Squadron (55 CSS), 55th Wing, Air Combat Command (ACC), Offutt AFB NE provides operational and software support.

1.1.2. Document Responsibility. The Commander, 55th Computer Systems Squadron, is the office of collateral responsibility for this instruction. Address questions to:

55 CSS

ATTN: Network Security Manager

201 Lincoln Highway, Suite 206

Offutt AFB, NE 68113-2040

1.2. Terminology.

1.2.1. Accreditation. Formal declaration by the designated approval authority (DAA) that an automated information system (AIS) is approved to operate in a particular security mode using a prescribed set of safeguards and controls.

1.2.2. Certification. Comprehensive evaluation of the technical and non-technical security features and countermeasures of an AIS to establish the extent to which a particular design and implementation meet a set of specified security requirements.

1.2.3. Security Categories. A grouping of classified or sensitive, but unclassified information to which an additional restrictive label is applied to signify that personnel are granted access to the information only if they have access approval (e.g., formal access approval). Examples include proprietary, for official use only (FOUO), Privacy Act, North American Treaty Organization, and compartmented information.

1.3. References and Acronyms. See **Attachment 1**.

2. Network Security Program Responsibilities.

2.1. Authority And Organization. HQ AFSPC is responsible for all security issues of the network. Actual development, execution, and monitoring of the Network Security Program are the responsibility of the Commander, 55 CSS, and the Network Security Manager (NSM). *NOTE*: See **Attachment 2** for diskette information and labeling instructions.

2.2. DAA.

2.2.1. TOP SECRET (TS) - General Service (GENSER). HQ AFSPC is the DAA for TS-GENSER. Responsibility includes all operational, configuration, and security issues impacting the SACCS-DTS Network either through direct processing or interface with other systems. The DAA for the SACCS-DTS Network will be the Director, Communications-Computer Systems (HQ AFSPC/SC). The HQ AFSPC point of contact (POC) for SACCS-DTS issues will be Systems Management Division, Communications-Computer Directorate (HQ AFSPC/SCMB).

2.2.2. Single Integrated Operation Plan - Extremely Sensitive Information (SIOP-ESI): Joint Staff, Pentagon, is the DAA for systems processing SIOP-ESI materials and information. The

DAA for SIOP-ESI approval is the Vice Director, Joint Staff (VDJS). The Joint Staff POC for SACCS-DTS issues will be Joint Staff, Systems Security Office (JS DOM/JSSO).

2.3. MAJCOMs. Other MAJCOMs using the SACCS-DTS Network will comply with the requirements of this instruction. Each MAJCOM will designate an action officer as a POC for SACCS users within their command. Notify HQ AFSPC/SCMB and the Network Manager (NM), (55 CSS/CC) SACCS/NM of SACCS POCs.

2.4. Network Operations. The Commander, 55 CSS, is responsible for the overall operation of the SACCS-DTS Network, including establishment and administration of the Network Security Program. The responsibilities include:

2.4.1. Appoint the NSM. The appointment letter will include name, rank, and duty title. Provide the appointment letter to the DAA at the MAJCOM and Joint Chiefs of Staff (JCS) level. The NSM must have direct access to the DAA and the Commander, 55 CSS, and be knowledgeable in computers, computer communications, computer security, and network security.

2.4.2. Establish a comprehensive Network Security Plan.

2.4.3. Perform a risk analysis of the SACCS-DTS Network at 3 year intervals. Identify and document all assumptions and constraints associated with the network. Review and update the risk analysis on an annual basis or when major configuration changes are made.

2.4.4. Obtain DAA approval from the lead command and JCS level for the network to process up to and including TOP SECRET/SIOP-ESI information.

2.4.4.1. Provide JCS with written certification that the SACCS-DTS Network meets security requirements of a multi-level secure system.

2.4.4.2. Maintain and comply with the requirements of the Continuing Security Certification and Accreditation Plan (CSCAP).

2.4.5. Direct a preliminary inquiry into each reported security incident involving the network. Ascertain the extent of the incident, refer it to the appropriate agency for action, and assist in the investigation. Coordinate with the investigating agency to identify and implement necessary changes to prevent reoccurrence.

2.5. NSM. The NSM is responsible for development, implementation, and direction of the Network Security Program. The security program relates to day-to-day operations, configuration management, and systems integration. The NSM will:

2.5.1. Be sure to fill the following computer security positions:

2.5.1.1. Network security officer (NSO) for each SACCS-DTS functional area (FA) with accountable processors, subnet communications processor (SCP), and base communications processor (BCP).

2.5.1.2. Terminal Area Security Officer (TASO) for each SACCS-DTS FA with non-accountable processors, aircraft wing command post (AWCP), missile base communications processor (MBCP), high frequency single side band (HFSSB), and collocated user terminal unit (CUTE).

2.5.1.3. Computer Systems Security Officer (CSSO) for each external system interfacing with the SACCS-DTS Network.

2.5.1.4. CSSO for the Computer Program Maintenance Facility (CPMF).

2.5.1.5. TASO for each CPMF remote terminal area.

2.5.2. Approve network security procedures to include local procedures established by NSOs, CSSOs, and TASOs within the SACCS-DTS Network.

2.5.3. Monitor activities on the network, using audit capabilities, to verify compliance with established security procedures.

2.5.4. Perform initial evaluation of security problems. If necessary, recommend to the DAA that access be denied to the network (including disconnection of the interface systems) while problems are being evaluated. Report problems and findings to the Commander, 55 CSS, and the DAA.

2.5.5. Review changes or modifications to network configuration or components to verify the integrity of network security features.

2.5.6. Review external interface accreditations and coordinate with the system CSSO to ensure network security integrity while connected to the SACCS network.

2.5.7. Document and report any identified network deficiencies to the Commander, 55 CSS and the DAA.

2.5.8. Chair the SACCS-DTS Security Working Group (SSWG). Coordinate certification and accreditation activities.

2.5.9. Be sure accreditation information is entered into the Information Processing Management System (IPMS).

2.6. NSO, SACCS-DTS Network. The commander responsible for the operation of each SCP and BCP will appoint a primary and alternate NSO. Forward a copy of the appointment letter to the NSM. The NSO is responsible for the security program at their FA and will be on duty or on call whenever the SACCS-DTS Network is in operation. The SACCS DTS NSO performs the duties specified for the computer security manager (CSM) in Air Force Systems Security Instruction (AFSSI) 5102, *The Computer Security (COMPUSEC) Program,* with the following specifications and additions:

2.6.1. Establish and enforce formal security operating procedures. Forward security procedures to the NSM for review and approval. Security procedures will support the Network Security Plan, and include as a minimum:

2.6.1.1. Physical Security.

2.6.1.2. Communications Security (COMSEC).

2.6.1.3. Emission Security (EMSEC).

2.6.1.4. Information Security.

2.6.1.5. Personnel Security.

2.6.1.6. Computer virus contingency plan (include backup and recovery).

2.6.1.7. Diskette Control.

2.6.1.8. Procedures for changes, modifications, or maintenance in system configuration or components.

2.6.1.9. Security awareness and training for users and staff.

2.6.1.10. Establish security incident and reporting policy and procedures.

2.6.2. Monitor security related network activities at the SCP or BCP.

2.6.3. Perform initial evaluation of any security problem or incident at the FA. Advise the DAA through the NSM if you recommend denial of access to a node, local CUTE, or external interface to the network. Report security problems immediately to the NSM and update the NSM on developments and findings relating to the security incident. Advise the NSM on developments and any other security related issues affecting the SCP or BCP.

2.6.4. Make sure only authorized personnel have access to terminals and associated hardware. Develop local procedures to ensure all local users of the SACCS network receive an initial network security briefing prior to access to the network. Document the briefing and maintain records on file.

2.7. TASO, SACCS-DTS Network. The officer-in-charge (OIC) responsible for the operation of each non-accountable processor (MBCP, HFSSB, AWCP, hardened user terminal element (HUTE), and rapid engagement and combat targeting (REACT) test sites) will appoint a primary and alternate TASO. The alternate TASO may be the controller or missile crew member on duty at the terminal. Forward a copy of the appointment letter to the NSM. The TASO is responsible for the security program at their facility, and will be on duty or on call whenever the SACCS-DTS Network is in operation. TASOs perform duties as described in AFSSI 5102 with the specifications and additions as listed in paragraph 2.6, above.

2.8. CSSO, External Interface Systems. The commander responsible for the operation of each external system that interfaces with the SACCS-DTS Network will appoint a primary and alternate CSSO. Forward a copy of the appointment letter to the NSM. The CSSO, External Interface Systems, will be the primary POC for the NSM to coordinate security issues concerning the interface system and the SACCS-DTS Network. In addition to the duties prescribed in AFSSI 5102, CSSOs for external interfaces must:

2.8.1. Establish and enforce local security operating procedures as necessary to comply with the SACCS-DTS Network Security Plan. Forward applicable security and operational procedures to the NSM for review and approval.

2.8.2. Review changes or modifications to interface system configuration or components with the NSM to verify the integrity of network security features and interface functionality.

2.8.3. Review and coordinate interface system accreditations with the NSM to ensure network security integrity while interface systems are connected to the SACCS-DTS Network. Develop, coordinate, and update memorandums of agreement between the interface system and the SACCS-DTS Network as necessary.

2.8.4. Document and report any identified security deficiencies, security incidents, or problems to the NSM.

2.8.5. Perform initial evaluation of security problems or incidents relating to the interface with the SACCS-DTS Network. If necessary, recommend to the applicable DAA if denial of access to the interface system and/or the SACCS-DTS Network is necessary (including the disconnection of the

interface system). Update the NSM on developments and findings relating to the security incident.

2.9. Network Operations Personnel. Network operations personnel operate the primary SCP at Offutt Air Force Base. Duty positions include:

2.9.1. Message Service Center (MSC) Operator: The MSC operator will monitor the MSC terminal and associated printer for system and user generated notifications. Notifications indicate potential impacts to the security and integrity of network operations. The MSC operator will report any security notifications to the NSO, provide periodic updates, and initiate appropriate corrective action.

2.9.2. Network Quality Control Center (NQCC) Operator: The NQCC Operator will monitor indications of network problems, either hardware or software. The NQCC Operator will report any security notification to the NSO and the chain of command. The NQCC Operator will compile notification statistics and provide any necessary historical data to support problem investigation and resolution.

2.9.3. Switch Operating Position (SWOP) Operator: The SWOP operator will monitor the SWOP for indication of system problems and report any occurrence to the NSM and the chain of command. At the direction of the NM or NSM, the SWOP operator will perform actions necessary to deny access to the network by "calling down" appropriate lines, local CUTEs, and printers.

2.10. Hardware And Firmware Support Personnel. Hardware and firmware support personnel include everyone involved with acquisition, maintenance, upgrade, and replacement of SACCS-DTS hardware. All maintenance personnel must comply with security procedures and requirements in order to maintain network integrity. The primary responsibility for hardware/firmware management rests with the SACCS Program Manager Sacramento Air Logistics Center (SM-ALC/LHO). Local responsibility is delegated to the Network Hardware Functional Manager (NHFM) at each FA.

2.10.1. NHFM: The senior maintenance technician at each SACCS FA will serve as the NHFM. The NHFM will:

2.10.1.1. Notify the NSM and NQCC of all modifications and upgrades prior to implementation.

2.10.1.2. Ensure all hardware support personnel comply with the Network Security Plan, local security procedures, and other applicable requirements.

2.10.1.3. Make sure all hardware identified for removal from the system is properly purged and declassified.

2.11. Network And System Users. A network or system user is any individual using the SACCS-DTS Network to transmit or receive messages, either through direct terminal or through interface systems.

2.11.1. Network users must comply with the Network Security Plan and local security procedures. All users must immediately report security violations, incidents, or problems to their security officer. The applicable security officer will immediately relay the report up the chain of command to the NSM, and begin preliminary inquiry into the situation.

2.11.2. Interface users must comply with all SACCS-DTS Network security requirements. Report security incidents and support investigative actions as requested by network security personnel.

3. Computer Program Maintenance Facility Security Responsibilities.

3.1. DAA.

3.1.1. TS-GENSER. HQ AFSPC is the DAA for TS-GENSER of the CPMF. Responsibility includes all operational, configuration, and security issues impacting the CPMF, either through direct processing or interface with other systems. The DAA for the CPMF is the Director, Communications-Computer Systems (HQ AFSPC/SC). The HQ AFSPC POC for SACCS-DTS issues is Systems Management Division, Communications-Computer Directorate (HQ AFSPC/SCMB).

3.1.2. SIOP-ESI. Joint Staff, Pentagon, is the DAA for all systems processing SIOP-ESI materials and information. The DAA for SIOP-ESI approval for CPMF Systems is the VDJS. The Joint Staff POC for CPMF issues will be Joint Staff, Systems Security Office (JS DOM/JSSO).

3.2. CSSO, CPMF. The Commander, 55 CSS, will appoint a primary and alternate CSSO for the CPMF. Forward a copy of the appointment letter to the NSM. The CSSO will be on duty or on call whenever CPMF systems are in use. The CSSO, CPMF, will perform all functions as listed in AFSSI 5102 with the following specifications:

3.2.1. Establish and enforce security procedures as in paragraph 2.6.1 through 2.6.1.8, above. In addition, include procedures for processor configuration for classified/unclassified processing (color change). Forward procedures to the NSM for review and approval.

3.2.2. Protect all system and user passwords according to AFSSI 5013, *Identification and Authentication*.

3.2.3. Establish and administer security training for all personnel requiring access to the CPMF (including remote terminal areas). Document and maintain records of all training on file. (*NOTE*: This may be delegated to the TASO.)

3.2.4. Serve as the office of primary responsibility (OPR) for all CPMF-related security issues.

3.3. TASO, CPMF. The commander or chief of each office operating remote terminals to the CPMF will appoint a primary and alternate TASO for their area. Forward a copy of the appointment letter to the NSM through the CSSO. The TASO, CPMF performs duties as listed in AFSSI 5102 with the following specifications:

3.3.1. Establish and enforce security procedures as in paragraph 2.6.1 through 2.6.1.8, above. Forward procedures to the CSSO for review and approval.

3.3.2. The TASO will be on duty or on call when CPMF remote terminals are in use.

3.3.3. Permit only authorized personnel access to terminal areas. If separated from the CPMF CSSO, administer security training for all personnel requiring access to CPMF systems. Document and maintain records of all training on file.

3.3.4. Enforce adherence to established security procedures.

3.3.5. Perform initial evaluation of security problems or incidents. Deny access as necessary, report all findings to the NSM. Report suspicious activity or non-compliance with security procedures to the NSM through the CSSO.

3.3.6. Report any suspicious activity or non-compliance with established procedures to the NSM and the facility manager.

3.4. Software Support Personnel. The Commander, SACCS C2 Systems Flight (55 CSS/CMT), serves as the Network Software Functional Manager (NSFM). Through sound configuration management, the NSFM ensures responsiveness and integrity of the software for the SACCS-DTS Network. All SACCS-DTS programmers, systems analysts, and configuration management personnel will comply with security procedures developed for the CPMF. All software support personnel will support the NSFM and network software security officer (NSSO) in development and maintenance of software security features.

3.5. NSSO. As the Network Manager, the Commander, 55 CSS, appoints the NSSO. Qualifications for the NSSO include familiarity with the SACCS-DTS security policy, through understanding of the Trusted Computing Base (TCB) software, and the TCB relation to security policy implementation. The NSSO also must be well versed in computer security and familiar with formal verification tools. The NSSO will:

3.5.1. Conduct formal verification of SACCS-DTS software. Accomplish this verification prior to each certification and accreditation of the network, or as directed by the DAA. Maintain the formal top level specifications.

3.5.2. Compare software design specifications to written source code to verify correlation between them.

3.5.3. Perform a software penetration test prior to each certification and accreditation cycle, or as directed by the DAA, NM, or NSM.

3.5.4. Assist programmers and configuration managers during the software development process.

3.5.4.1. Provide security input and recommendations to the requirements analysis team for the initial evaluation of software change projects.

3.5.4.2. Provide security input and recommendations to the programming team during the design review.

3.5.4.3. Review the documentation change request for security requirements and completeness

3.5.4.4. Conduct a trusted code review for all projects involving trusted code prior to building diskettes for each software release. Document and maintain the review, with copies of the applicable source units.

4. Network Security Procedures.

4.1. SACCS Security Working Group (SSWG). The SSWG provides continued security oversight of the network and it's security features. The SSWG reviews all system security policies, practices and plans; documents findings and addresses flaws, and provides recommendations. Specific duties of the SSWG include:

4.1.1. Serve as the OPR and focal point for planning, coordinating, and executing all activities relating to the on-going certification and accreditation of the SACCS-DTS Network. Advise and guide the Commander, 55 CSS, and the DAA on all matters related to security recertification.

4.1.2. Identify supporting requirements for security recertification to the appropriate agencies and offices for action.

4.1.3. Assemble and submit the recommendation package to the DAA for system accreditation.

4.1.4. Review and comment on the SACCS CSCAP.

4.1.5. Review all system design changes (hardware and software) to identify potential security vulnerabilities and impact.

4.1.6. Coordinate on security matters with agencies and offices not represented on the SSWG, including Defense Information Systems Agency (DISA) and contractors as necessary.

4.2. SSWG Membership. The following agencies or offices are members of the SSWG. Each member will support the tasks and responsibilities listed. The Network Security Manager, as Chairperson, may include other agencies as necessary for input to the needs of the SSWG.

4.2.1. Office of the Joint Chiefs of Staff (OJCS): Guide the SSWG on Department of Defense (DoD) and JCS requirements for the SACCS-DTS Network.

4.2.2. NSM. As Chairperson, SSWG, the NSM will:

4.2.2.1. Update and produce necessary plans, reports, and procedures to assist in the recertification effort.

4.2.2.2. Provide input on updated operational requirements.

4.2.2.3. Participate in technical evaluation of all security-relevant hardware and software.

4.2.2.4. Assist in security testing, verification, and correlation's where appropriate, or as directed by the DAA.

4.2.2.5. Maintain responsibility for operational software maintenance and modification during the continued operation of the network.

4.2.2.6. Maintain and revise all security related documentation and publications, including systems regulations and the CSCAP.

4.2.3. National Security Agency (NSA): Serve as the SACCS security advisor for HQ AFSPC and the OJCS.

4.2.4. Air Intelligence Agency (AIA):

4.2.4.1. For EMSEC considerations:

4.2.4.1.1. Provide guidance on COMSEC and EMSEC engineering and applications for the SACCS-DTS Network.

4.2.4.1.2. Provide an emanation security evaluation for SACCS-DTS, based on EMSEC test results obtained during previous system evaluations.

4.2.4.1.3. Provide an emanation security evaluation for facilities housing SACCS-DTS equipment and provide additional facility EMSEC testing as necessary.

4.2.4.2. For Security Management:

4.2.4.2.1. Provide technical service and support for managing SACCS-DTS security.

4.2.4.2.2. Provide (on request) implementation guidance and technical interpretation of automated data processing (ADP) security policies. Provide (on request) recommendations on hardware, software, physical, and procedural safeguards.

4.2.4.2.3. Assist the DAA in the review of risk analysis documentation.

4.3. Design Control Board (DCB). This board is the approval authority for all baseline change requests (BCR) to the SACCS-DTS Network. Functionally the DCB is an element of the Configuration Control Board and retains approval authority over all hardware, firmware, and off-line diagnostic changes. The NSM, with advisement from the NSSO for software issues, advises the DCB regarding possible security impacts of any proposed changes.

4.4. System Certification And Accreditation. Any system that processes or transmits classified data must, in the opinion of the data's owner, provide appropriate protection against unauthorized access or use. The certification and accreditation process encompasses every significant change and modification for the entire life-cycle of the system. Realistically, the process is a periodic review, unless driven by special conditions. The CSCAP is the certification and accreditation plan for the SACCS-DTS Network. As chairperson of the SSWG, the NSM monitors activities necessary for system certification and accreditation.

4.4.1. Accomplish a complete certification of the SACCS-DTS Network every 3 years. The SSWG completes all certification actions and forwards the package to the DAA for the SACCS-DTS Network. The Network DAA will, in turn, forward the package to JCS for approval to process SIOP-ESI. The certification package must meet the requirements of AFSSI 5024, *Certification and Accreditation,* and will include as a minimum:

4.4.1.1. Sensitivity and criticality assessment.

4.4.1.2. Risk assessment.

4.4.1.3. Economic assessment.

4.4.1.4. Security test and evaluation.

4.4.1.5. Formal verification of the TCB software.

4.4.1.6. Security procedures.

4.4.1.7. Summary of design changes.

4.4.2. Complete all actions so the Commander, 55 CSS, and the NSM receive the approved accreditation prior to the expiration of the previous certification/accreditation. Other situations that necessitate a complete certification include whenever:

4.4.2.1. A new external interface is added.

4.4.2.2. Adding a new trusted process.

4.4.2.3. The functionality of the network increases

4.4.2.4. Discovering a breach of security affecting the integrity of the system.

4.4.3. Prepare and forward a report of all security relevant changes to the DAA for the SACCS-DTS Network on an annual basis. The DAA reviews the report and then forwards it to JCS for further approval. The annual report will include, as a minimum:

4.4.3.1. All software changes to the TCB.

4.4.3.2. Security procedures and plans

4.4.3.3. Risk assessment

4.4.3.4. Risk analysis, updated to reflect the additional or updated assessment.

4.5. System Audits. The NSM performs system audits to verify secure operation of the system and support software. If the NSM discovers any irregularities, he or she begins an analysis to identify the problem and corrective actions necessary to resolve the situation. Explore all possible alternatives during the analysis. The NSM maintains historical records of audit problems and corrective actions. The NSM actively tracks open items and briefs the NM and SSWG on identified security deficiencies.

4.6. Personnel Security. The SACCS-DTS Network is accredited to process information up to and including TOP SECRET/SIOP-ESI. All accountable processors must be able to process traffic at the TOP SECRET/SIOP-ESI level. Clear all SCP operators and BCP management personnel to TOP SECRET/SIOP-ESI. Subscribing processors may be assigned a lower classification level. NSOs and TASOs will ensure their security procedures include comprehensive and clear actions to enforce personnel security actions. Permit access to the system only to personnel with the required security clearance and valid need-to-know. NSOs and TASOs must maintain close coordination with their unit security manager(s) to keep personnel security records and files current and accurate.

4.7. Physical Security. System users will implement physical security measures for all FAs of the SACCS-DTS Network.

4.7.1. The *minimum* physical security requirements for SACCS-DTS nodes are:

4.7.1.1. Each area containing a SACCS-DTS node must be authorized for open storage at the classification level of the processor.

4.7.1.2. Secure each accountable SACCS-DTS processor (SCP or BCP) as a restricted area. This means the terminal does not have to reside within a restricted area, but it must be afforded the protection of a restricted area when processing classified data.

4.7.1.3. Secure each non-accountable SACCS-DTS node as a controlled area.

4.7.2. NSOs or TASOs will develop and implement access procedures that address entry control, escort procedures, and system access authorization.

4.7.3. Unmanned Terminal Areas: Terminals in an unmanned area must be "powered down" by the appropriate SCP operator. Follow procedures detailed in **Attachment 3**. Include actions to secure classified output or data prior to leaving the terminal unattended.

4.8. Communications Security. Security of message traffic *within* the SACCS-DTS network is achieved by link encryption, employing data communication cryptographic devices. Proper cryptographic procedures are essential for data integrity and system operation. All personnel must also protect message traffic *outside* the system.

4.8.1. Protect all COMSEC code materials according to AFI 33-211, *Communications Security (COMSEC) User Requirements*.

4.8.2. Maintain a high level of COMSEC Awareness. Refer to **Attachment 4** for the critical information (CIs) for the SACCS-DTS Network. Incorporate on-going COMSEC awareness in the Security Awareness and Training Education (SATE) Program.

4.9. Emission Security (EMSEC). Systems processing or transmitting classified data must protect against interception of inadvertent emanations for the equipment. Comply with the requirements of AFI 33-203, *The Air Force Emission Security Program,* for SACCS-DTS network FAs. Conduct an EMSEC inspection annually, or if any conditions or factors used in the assessment or countermeasures review change.

4.10. Information Security. All network personnel must be familiar with the requirements concerning the handling, marking and storage of classified information. Incorporate proper classified handling in security procedures and SATE Training.

5. Computer Program Maintenance Facility Security.

5.1. Introduction. The security requirements of the CPMF are separate and distinct from the operational network, but of equal importance. The CPMF consists of the software test facility (STF), the development hosts, remote terminals, peripherals, and supporting facilities. The CPMF also includes the personnel, equipment, and other resources necessary to support software maintenance for the SACCS-DTS Network.

5.2. System Guidelines.

5.2.1. Development Host Processor. Dedicated to unclassified processing to support software development activities, maintain master level software libraries, and build operational load diskettes for distribution to field units. Security procedures cover the protection of sensitive unclassified data and the integrity of master libraries.

5.2.2. Classified Host Processor. This processor supports processing requirements associated with journal and dump analysis.

5.2.3. Software Test Facility (STF). The STF is extremely vulnerable to security incidents due to the high usage in both classified and unclassified modes. The CSSO, CPMF will ensure procedures cover classification mode changes, equipment configuration, and diskette handling. Operations, programmer, and tester personnel will comply with all security procedures at all times.

5.2.4. Development host and classified host processors can be connected to the STF. Procedures for equipment configuration will include verification of proper security levels on the STF prior to connection.

5.3. Procedures. Security procedures for systems that comprise the CPMF are subject to the same security constraints and procedures as the operational network. Unique requirements of CPMF systems are as follows:

5.3.1. System Certification And Accreditation. Accomplish a complete certification of the CPMF systems every 3 years. Comply with the requirements of AFSSI 5024, as for the operational network. The SSWG completes all certification actions and forwards the package to the DAA for approval. The network DAA will in turn forward the package to JCS for approval to process SIOP-ESI. Complete all actions so the NM and NSM receive the approved accreditation prior to the expiration of the previous certification/accreditation. Other situations that necessitate a complete certification include when:

5.3.1.1. Adding a new external interface to CPMF system(s).

5.3.1.2. Adding a new trusted process.

5.3.1.3. The functionality of the CPMF increases.

5.3.1.4. Discovering a breach of security affecting the integrity of the system.

5.3.2. System Audits. The NSM performs system audits and spot checks to verify secure operation of the system and support software. If the NSM discovers any irregularities, he or she begins an analysis to identify the problem and corrective actions necessary to resolve the situation. Explore all possible alternatives during the analysis. The NSM maintains historical records of audit problems and corrective actions. The NSM actively tracks open items and briefs the NM and SSWG on identified security deficiencies.

5.3.3. Personnel Security. CPMF systems (STF and Host III) are accredited to process information up to and including TOP SECRET/SIOP-ESI. Clear all SACCS Operation Flight (55 CSS/ CMO) operators and CMT programmers to TOP SECRET/SIOP-ESI. The NSM will ensure security procedures include comprehensive and clear actions to enforce personnel security actions. Permit access to the system only to personnel with the required security clearance and valid need-to-know. Maintain close coordination with unit security manager(s) to keep personnel security records and files current and accurate.

5.3.4. Physical Security. Implement physical security measures for all FAs of the CPMF.

5.3.4.1. Each area containing a classified processor must be authorized for open storage at the classification level of the processor.

5.3.4.2. Secure each accountable CPMF processor within a restricted area.

5.3.4.3. Each CPMF CSSO or TASO will develop and implement access procedures.

5.3.4.3.1. If the owner/user is responsible for entry control, develop and implement security procedures for entry control to the facility.

5.3.4.3.2. Develop and implement security procedures to verify authorization prior to access to a CPMF terminal or system.

5.3.4.3.3. Establish clear escort guidelines and responsibilities.

5.3.5. EMSEC. Comply with the requirements of AFI 33-203 for CPMF Systems. Conduct a EMSEC inspection annually, or if any conditions or factors used in the assessment or countermeasures review change.

5.3.6. Information Security. All CPMF personnel must be familiar with the requirements concerning the handling, marking and storage of classified information. Incorporate proper classified handling in security procedures and SATE Training.

6. Control of Classified Media.

6.1. Classified Accountability. Each SACCS-DTS FA is categorized as a telecommunications facility (TF) as defined in AFI 31-401, *Managing the Information Security Program*. Control message copies as classified working papers unless retained longer than 30 days. Control classified diskettes as listed below.

6.1.1. Record Copy Disposition. SACCS-DTS may transmit any range of classified messages from UNCLASSIFIED to TOP SECRET. Some of these messages may be printed without down-grading instructions. In this case, treat messages as classified working papers and protect according to AFI 31-401. Control any permanently retained message according to AFI 31-401.

6.2. Media Management, Operational Network. Maintain software and operational information for the SACCS-DTS on eight-inch diskettes. Registered mail or United Parcel Service (UPS) is used to ship diskettes. The inner wrapping of all shipments is sealed with the SACCS-DTS logo imprinted tape.) Proper handling and protection of the media are critical to the continued and secure operation of the system.

6.2.1. General Handling Guidelines. Protect the diskettes from extreme temperatures, magnetic forces, bending, and contaminants. Do not touch exposed surfaces on the diskette. When storing diskettes, keep the diskette in the protective jacket when not in the disk drive. Failure to follow these instructions could lead to damaged media.

6.2.2. Diskette Classification. Once placed in the processor, classify and control **ALL** diskettes at the security level of the processor. Regardless of classification, account for all diskettes. Units will implement local procedures to account for UNCLASSIFIED and SECRET diskettes. Account for TOP SECRET diskettes according to AFI 31-401.

6.2.2.1. Initial Program Load (IPL) Diskettes. IPL diskettes are UNCLASSIFIED when shipped from 55 CSS/CMOL (SACCS Library). Retain IPL diskettes as directed by the current Version Description Document, paragraph 2.6. Destroy all other IPL diskettes according to paragraph 6.2.8, below.

6.2.2.2. System Diskettes (Menu, Journal, Dump). System diskettes are UNCLASSIFIED when shipped from 55 CSS/CMOL (SACCS Library). Retain diskettes for reuse within the same processor until the diskette is unusable. Once unusable, destroy the diskette according to paragraph 6.2.8, below.

6.2.3. Top Secret Control Account. Any FA with a processor at the TOP SECRET level will establish a Top Secret Control Account according to AFI 31-401. Establish written procedures to track access, accountability, and tracking of diskette issue. Use local forms in place of individual AF Form 143, **Top Secret Register Page**. Inventory diskettes on an annual basis as required by the above directives.

6.2.4. Diskette Retention. Retain and reuse diskettes for as long as possible. Reuse is encouraged within the parameters of security requirements and operational considerations.

6.2.4.1. Dump Diskettes. Retain Dump diskettes for a minimum of 10 days. If not required for dump analysis, reuse dump diskettes as necessary. If dump analysis is necessary, NQCC will contact the affected site and arrange for remote dump or shipment of the dump diskette.

6.2.4.2. Journal Diskettes. BCPs will retain Journal diskettes for 10 days. SCPs will retain Journal diskettes for 30 days. If not required for system analysis or message tracking, reuse journal diskettes as necessary. If journal analysis is necessary, NQCC will contact the affected site and arrange for remote dump or shipment of the journal diskette.

6.2.4.3. Diagnostic /Journal Index/Empty Diskettes. Diagnostics and Journal Index diskettes are shipped formatted with specific files. System configuration and file structure prevent these diskettes from containing any information higher that UNCLASSIFIED/FOUO. Retain until

no longer usable or replaced. Destroy according to paragraph 6.2.8, below

6.2.5. Diskette Labeling. Label diskettes according to AFI 31-401. When shipped, CMO labels diskettes with identifying serial numbers and a diskette name. Do not remove this label. Include labels or markings for warning notices (i.e., Restricted Data, SIOP, etc.) on those diskettes that contain such information.

6.2.6. Diskette Analysis. If there is a need to analyze a dump diskette or journal diskette, NQCC will make arrangements for remote dump action and or shipment of the diskette. Missile crews will **not** process remote dump actions from the launch control center (LCC), but return dump diskettes to the issuing agency (DO22) for remote dump processing or shipment. When shipping diskettes, comply with the requirements of AFI 31-401 for handling classified media.

6.2.7. Diskette Destruction.

6.2.7.1. Destroy classified media according to AFSSI 5020, *Remanence Security*. **NOTE:** Destroy the diskettes locally. Do NOT return media to SACCS Library for destruction*.*

6.2.7.2. Document destruction of diskettes according to AFI 31-401. Forward an information copy of destruction records to 55 CSS/CMOL (SACCS Library) for accountability purposes.

6.3. Media Management, CPMF. Processors within the CPMF operate in a controlled environment from UNCLASSIFIED to TOP SECRET. In order to provide extensive testing configurations, the CPMF provides capabilities to override software and hardware constraints. Therefore, control all diskettes, regardless of the file types/names, as follows:

6.3.1. Mark and control all diskettes used in the CPMF for unclassified system development and test as UNCLASSIFIED, indicating their use in a "Black" system only.

6.3.2. Mark and control all diskettes used in the CPMF when operating at the classified level as TOP SECRET/SIOP-ESI, indicating their use in a "Red" system only.

6.3.3. This requirement does not preclude different processors in the STF from running at different classification levels as long as they are isolated from one another by software and/or physical means.

WILLIAM J. DONAHUE,   Lt General, USAF
Director, Communications and Information

Attachment 1

GLOSSARY OF REFERENCES, ABBREVIATIONS, AND ACRONYMS

References

AFPD 33-1, *Command, Control, Communications, and Computer (C^4) Systems*

AFPD 33-2, *Information Protection*

AFI 31-101, *The Physical Security Program*

AFI 33-203, *The Air Force Emission Security Program*

AFI 31-209, *The Air Force Resource Protection Program*

AFI 31-401, *Managing the Information Security Program*

AFI 33-211, *Communications Security (COMSEC) User Requirements*

AFSSI 5020, *Remanence Security*

AFSSI 5024, *The Certification and Accreditation (C&I) Process System Certification Guide*

AFSSI 5013, *Identification and Authentication*

AFSSI 5102, *The Computer Security (COMPUSEC) Program*

Significant References

Chairman, Joint Chiefs of Staff Instruction (CJCSI) 3132.01(S), *Safeguarding the Single Integrated Operational Plan* (U)

AFMAN 33-229, *Controlled Access Protection*

AFSSI 5021, *Vulnerability and Incident Reporting*

AFSSM 5018, *Risk Analysis Guide*

AFSSM 5023, *Viruses and Other Forms of Malicious Logic*

Abbreviations and Acronyms

AFSSI—Air Force Systems Security Instruction

AFSSM—Air Force System Security Memorandum

AIS—Automated Information System

AWCP—Aircraft Wing Command Post (Non-Accountable Processor)

BCP—Base Communications Processor (Accountable Processor)

COMSEC—Communications Security

CPMF—Computer Program Maintenance Facility.

CSCAP—Continuing Security Certification and Accreditation Plan

CSS—Computer Systems Squadron

CSSO—Computer Systems Security Officer

CUTE—Collocated User Terminal Element

DAA—1) Designated Approval Authority 2) Display Alternate Area Routing Lists (JP 1-02)

DTS—Data Transmission Subsystem

ESI—Extremely Sensitive Information

FA—Functional Area

FOUO—For Official Use Only

HFSSB—High Frequency Single Side Band

HUTE—Hardened User Terminal Element (Non-Accountable Processor)

IPL—Initial Program Load

JCS—Joint Chiefs of Staff

MBCP—Missile Base Communications Processor (Non-Accountable Processor)

MSC—Message Service Center

NHFM—Network Hardware Functional Manager

NM—Network Manager

NQCC—Network Quality Control Center

NSM—Network Security Manager

NSO—Network Security Officer

NSSO—Network Software Security Officer

OJCS—Office of Joint Chiefs of Staff

OPR—Office of Primary Responsibility

POC—Point of Contact

SACCS—Strategic Automated Command Control System

SATE—Security Awareness and Training Education

SCP—Subnet Communications Processor (Accountable Processor)

SIOP—Single Integrated Operation Plan

SSWG—SACCS-DTS Security Working Group

STF—Software Test Facility

TASO—Terminal Area Security Officer

TCB—Trusted Computing Base

VDJS—Vice Director, Joint Staff

Attachment 2

DISKETTE INFORMATION AND LABELING INSTRUCTIONS

A2.1. General Information. This attachment consists of three sections: General Information, UNCLASSIFIED Diskette Labeling Guidance, and CLASSIFIED Diskette Labeling Guidance.

A2.1.1. IPL Diskettes. The total quantity of IPL diskettes at each FA will depend on the releases and modifications. Implementation instructions in the software version description (SVD) will include which IPL diskettes to retain and which to destroy. Store archived IPL diskettes (that is, other than the current release) in a separate location to preclude inadvertent use.

A2.1.2. Support Diskettes. Distribution of support diskettes to each site depends on the type of FA(s) installed at the location. Table A2.1, below, lists the minimum requirements for each type of FA. The listings for supporting agencies (DO22 or SCUC) show the number of diskettes maintained in stock for replacement of damaged or recycled HUTE and MBCP diskettes. Each FA operational manager is responsible to maintain the minimum quantity of diskettes at their FA. Request additional diskettes from 55 CSS/CMO as necessary.

Table A2.1. Minimum Diskette Requirements for Each FA.

FA	MENU	DUMP	DIAG 3	EMPTY	JNL INDEX	JOURNAL	DIAG 1	DIAG 2	D28M1X
HUTE	2	3	1						
MBCP	2	3	1						
DO22	40	100	20						
HFSSB	6	8	3						
AWCP	10	20	3						
BCP	10	30	3	6	10	100			
B SCP	6	20		15	10	1000	3	3	40
O SCP*	6	20		40	10	4000	3	3	40
LVR	3	3	3						
MMTS	3	3	3	5					
CMTS	3	2	3	3			3	3	20
CRA	2	2	2	2			1	1	20

*O SCP also includes 500 DPSRCVY (DPS Recovery) diskettes, as well as CPMF diskettes.

A2.1.3. If a diskette fails, issue a replacement from the supporting agency, and request replacements from 55 CSS/CMO. Destroy all failed or unusable diskettes locally. Once installed in the SACCS-DTS processor, mark and control the diskette at the level of the processor.

A2.1.4. Do not use maintenance set diskettes (LVR, CMTS, MMTS, and CRA) in any equipment other than maintenance sets. If any maintenance set diskette is used in an on-line system, mark and control according the classification level of the processor.

A2.1.5. Unique diskettes used to restore files to the hard disk at SCPs are not shown in Table A2.1. As originally issued, these diskettes were unclassified. Once inserted into the processor, mark and control as TOP SECRET/SIOP-ESI.

A2.1.6. **CAUTION:** *Do not write on labels affixed to a diskette using any ball-point pen or pencil. Hard point objects will cause diskette damage and subsequent equipment failure. Do not cover exposed portion of the diskette media with labels, as this disrupts the media operation.*

Avoid touching exposed portions of the diskette media. Do not remove manufacturers or disk identification labels. For Journals, Menu, and Journal Index (Jnlindex) files, cover the write inhibit slot with a tab if the slot exists on single density (Type 2) diskettes before use in the main storage unit (MSU).

A2.2. Unclassified Diskette Labeling: All diskettes are UNCLASSIFIED prior to being used in the processor. Refer to Figure A2.1 for diskette label positions. Paragraph A2.2.1 shows the label format for Unclassified, Journal, Menu, and Dump diskettes prior to their use.

Figure A2.1. Diskette Label Positions.
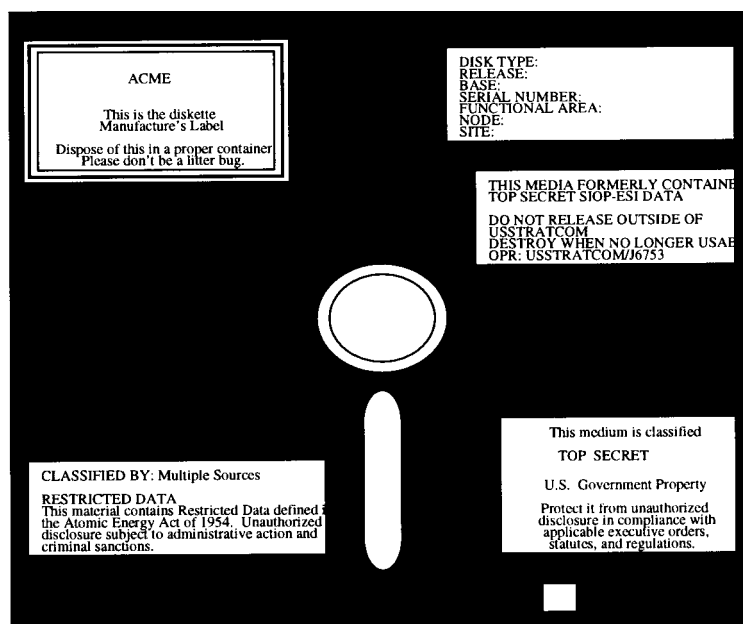
A2.2.1. IPL, Diagnostics, Empty, Jnl Index Diskette Label.

DISK TYPE:

RELEASE:

BASE:

SERIAL NUMBER:

FUNCTIONAL AREA:

NODE:

SITE:

Table A2.2. Journal, Dumpfile, and Menu Diskette Labels.

MENUSERIAL NBR:	DUMPFILESERIAL NBR:	JOURNALSERIAL NBR:

A2.3. Classified Labeling.

A2.3.1. The system is accredited to process multi-level security classifications. Once used, mark and control diskettes as classified media. Control all diskettes at the classification level of the processor.

A2.3.2. Place the appropriate label from paragraph A2.2.2 in position #1 on the diskette. Place the appropriate classification (SF 706, **Top Secret ADP Media Classification Label;** SF 707, **Secret ADP Media Classification Label**; and SF 708, **Confidential ADP Media Classification Label**) label in position shown in paragraph A2.3.3.

A2.3.3. Sample "Classified By" Label.

CLASSIFIED BY: Multiple Sources

RESTRICTED DATA

This material contains Restricted Data defined in

the Atomic Energy Act of 1954. Unauthorized

disclosure subject to administrative action and

criminal sanctions.

A2.3.4. Include the "CLASSIFIED BY" and "RESTRICTED DATA" label shown in paragraph A2.3.3 in position #3. Each unit will implement local measures in order to minimize the work load in labeling diskettes.

A2.3.5. Any diskette that contains (or did contain) TOP SECRET/SIOP-ESI data requires USSTRATCOM Form 148, SIOP Data Label (paragraph A2.3.5.1) on the diskette. The 55CSS/CMO will ship unaffixed USSTRATCOM Form 148s with formatted, empty diskettes. Whenever a Journal, Menu, or Dumpfile diskette is used in a TOP SECRET processor, place the USSTRATCOM Form 148 on the diskette. *Once placed on the diskette, **do not remove** the form for any reason, **regardless of classification**.* If you need additional forms, contact 55 CSS/CMO.

A2.3.5.1. USSTRATCOM Form 148.

THIS MEDIA FORMERLY CONTAINED

TOP SECRET SIOP-ESI DATA

DO NOT RELEASE OUTSIDE OF

USSTRATCOM

DESTROY WHEN NO LONGER USABLE

OPR: USSTRATCOM/J6753

Attachment 3

UNMANNED COLLOCATED USER TERMINAL ELEMENT (CUTE) PROCEDURES

A3.1. SACCS-DTS FA. Any SACCS-DTS FA that is not staffed on a 24-hour basis must implement procedures for activation and deactivation of the CUTE during periods the terminal is unattended. The office will submit a letter to the parent SCP, identifying personnel authorized to activate and deactivate the terminal. The letter will include, as a minimum:

A3.1.1. Name, rank, and social security number.

A3.1.2. Birth date, office symbol, and telephone number.

A3.1.3. Normal duty hours of the office.

A3.2. Activation of a CUTE.

A3.2.1. During Duty Hours. To bring an off-line terminal on-line, the operators will contact the SCP Operator, and identify themselves using data from the authorization letter. The SCP Operator annotates the name in the master station log, and then takes the appropriate actions to bring the CUTE on-line.

A3.2.2. During Non-Duty Hours. To bring an off-line terminal on-line during non-duty hours, the operator will contact the SCP operator, and identify themselves using data from the authorization letter. The SCP operator will verify the requester's identity and access level with the duty controller at that installation. Once verified, the SCP operator annotates the name in the master station log, and then takes the appropriate actions to bring the CUTE on-line.

A3.3. Deactivation of a CUTE. To take an on-line terminal off-line, the CUTE operator will contact the SCP operator, and identify themselves using data from the authorization letter. The SCP operator will verify the request by call back to the telephone number listed on the authorization letter for that CUTE. The SCP operator annotates the name in the master station log, and takes the appropriate actions to take the CUTE off-line.

A3.4. Protection of Classified Materials. Each agency operating CUTEs under these procedures will implement procedures to:

A3.4.1. Purge the area and secure any classified materials.

A3.4.2. Make sure of the security of message traffic while the CUTE is unattended.

Attachment 4

CRITICAL INFORMATION LISTING - SACCS-DTS NETWORK

A4.1. Systems:

A4.1.1. Status and capabilities of assigned computer systems.

A4.1.2. Faults or weaknesses in hardware, software, or message processing capabilities in the SACCS-DTS Network, related systems or external interface systems.

A4.1.3. Times of classified processing, and levels processed.

A4.1.4. Scheduled or unscheduled systems down-time.

A4.1.5. Communications links.

A4.2. Output:

A4.2.1. Testing of future releases, results of on-line testing (See Note below).

A4.2.2. Remote Dump Processing.

A4.2.3. Periodic Updates.

A4.2.4. Source Code and output products.

A4.2.5. Individual Elements of Software Release Implementation (Version, Time, Date).

A4.3. Operations:

A4.3.1. Status of mission activities during normal operations.

A4.3.2. Increased operational or exercise activities.

A4.4. Resources:

A4.4.1. Manning.

A4.4.2. Training deficiencies.

A4.4.3. Status of equipment and/or budget.

NOTE:

Testing is unclassified unless data reveals weakness or limitations of the system. Classify such data as SECRET, Operating Agency's Determination Required (OADR). For further information, refer to the SACCS-DTS Security Classification Guide, 15 Oct 91.